

Re: Is there a way to query Security Event Log with Filter in C#?

Source:

<http://www.tech-archive.net/Archive/DotNet/microsoft.public.dotnet.languages.csharp/2007-01/msg00537.html>

- *From:* Pucca <Pucca@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Thu, 4 Jan 2007 12:29:00 -0800
-

Thanks Peter. I tried it in my code but it's just exiting when it reaches the statement `mos.get()`. Can you see what's wrong here? Also, where can I look up syntax format and the properties names for the Security log? Thanks.

```
private void GetLog()
{
//string SomeDateTime = "20060101000000.000000+000";
//string Query = String.Format("SELECT * FROM Win32_NTLogEvent WHERE
Logfile = 'Security' AND TimeGenerated > '{0}'", SomeDateTime);
string Query = String.Format("SELECT * FROM Win32_NTLogEvent WHERE
Logfile = 'Security'");

object o;
string name;
try
{
ManagementObjectSearcher mos = new ManagementObjectSearcher(Query);
foreach (ManagementObject mo in mos.Get())
{
foreach (PropertyData pd in mo.Properties)
{
o = mo[pd.Name];
if (o != null)
{

//Console.WriteLine(String.Format("{0}: {1}", pd.Name,
mo[pd.Name].ToString()));
}
}
}
mos.Dispose();
}
catch (Exception e)
{
MessageBox.Show(e.Message);
}
}
```

Re: Is there a way to query Security Event Log with Filter in C#?

```
}  
--
```

Thanks.

"Petar Repac" wrote:

Hi !

You can try WMI query for this.

Example that filters event log by LogFile and TimeGenerated.

```
using System;  
using System.Collections.Generic;  
using System.Text;  
using System.Management;  
  
namespace QueryEventLog {  
  
    class Program {  
        static void Main(string[] args) {  
            string SomeDateTime = "20070101000000.000000+000";  
            string Query = String.Format("SELECT * FROM Win32_NTLogEvent  
            WHERE Logfile = 'Application' AND TimeGenerated > '{0}'", SomeDateTime);  
            ManagementObjectSearcher mos = new ManagementObjectSearcher(Query);  
            object o;  
  
            foreach (ManagementObject mo in mos.Get()) {  
  
                Console.WriteLine("////////////////////////////////////");  
                foreach (PropertyData pd in mo.Properties) {  
                    o = mo[pd.Name];  
                    if (o != null) {  
                        Console.WriteLine(String.Format("{0}: {1}", pd.Name,  
                        mo[pd.Name].ToString()));  
                    }  
                }  
  
                Console.ReadLine();  
            }  
        }  
    }  
}
```

Hope it helps.

Petar Repac

Re: Is there a way to query Security Event Log with Filter in C#?

Pucca wrote:

Thank you Jani. I'm already using the eventLog class and processing each log entry and filtering them in my C# code (vs2005, .net2.0) and then place the filtered / qualified rows in to a dataset table.

The problem is this is taking a long time. It's taking 45 seconds just to read about 45k of entries(I get the entrycollection then use a logentry variable to read each one). Are there anyway to improve this?